2002 National Medicaid
HIPAA and MMIS Conference

EDS

HIPAA Security From Gap Analysis to Action Plan

Presented By: Mark L. Schuweiler
Director of Health Care Information Assurance
EDS Corporation

Agenda

- Communication isn’t what it used to be.
- Is HIPAA Security really secure?
- How do you measure HIPAA security compliance?
- What do you do if you are not compliant?
- Conclusions

Complex Security Issues

Private Network

- HMOs /Agency
- Employees
- Regional Centers
- Customer Help Desks

Public Internet

Intranet

Extranet or VPNs

Doctors

Patients

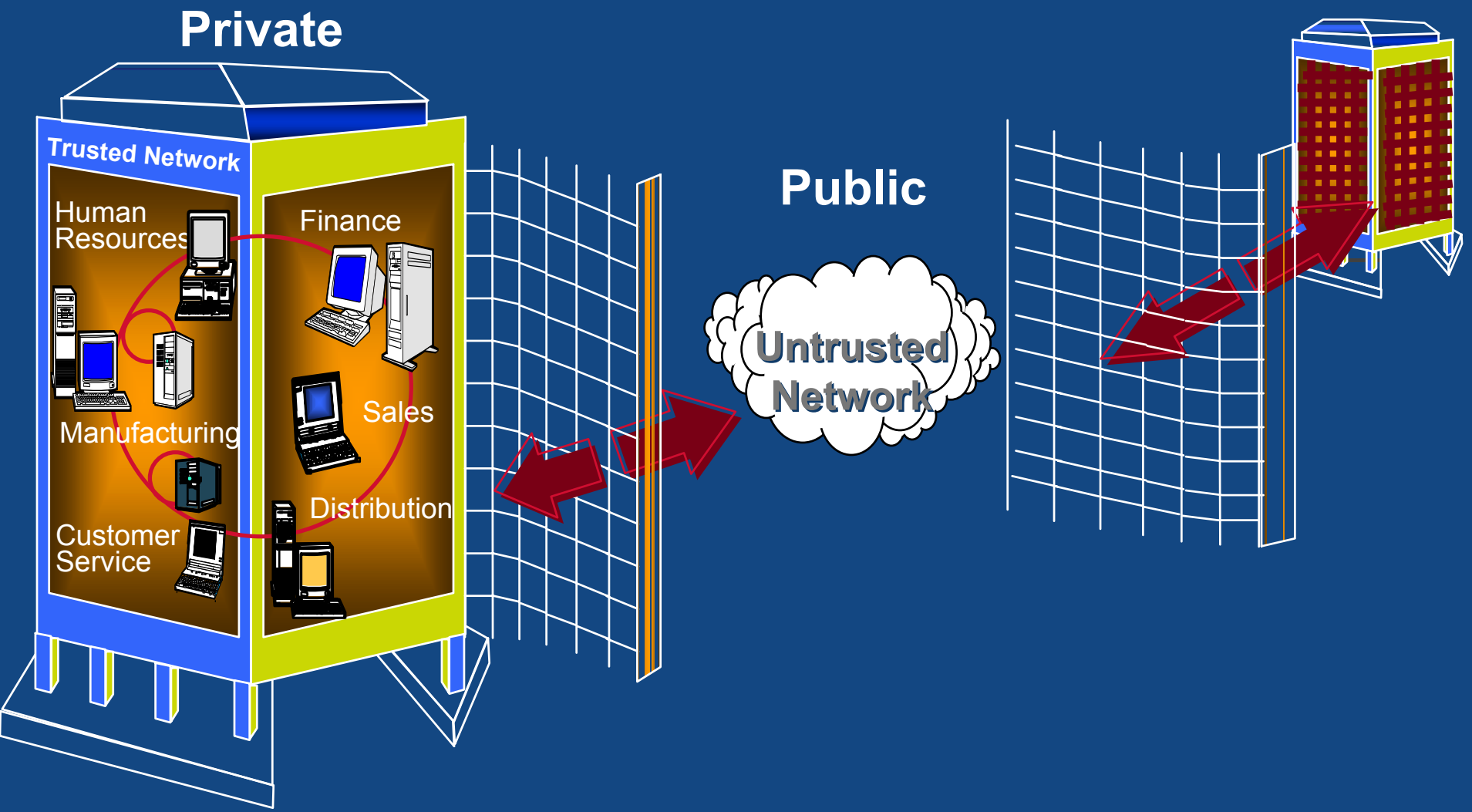
Insurance

Labs

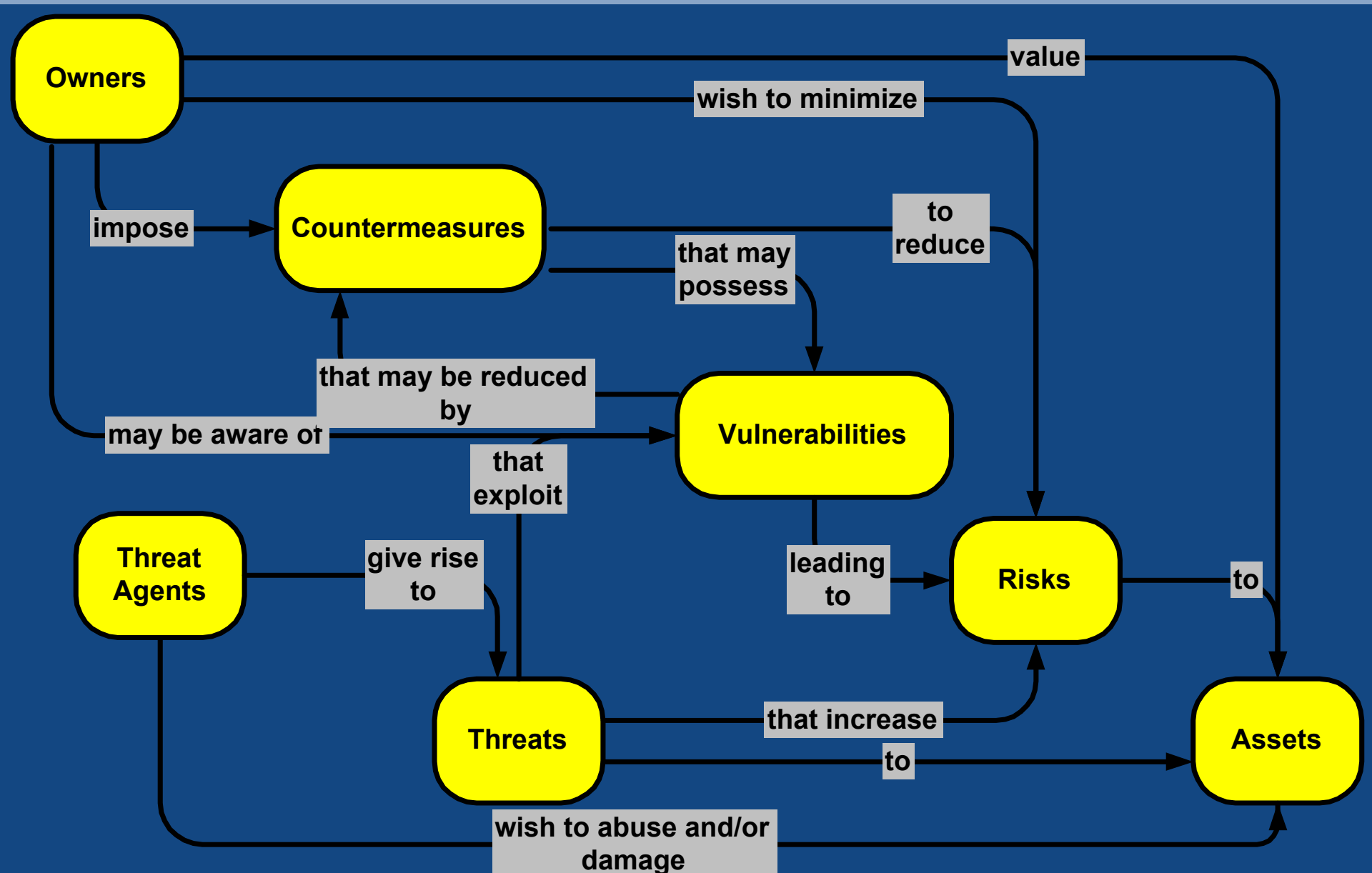
Clinics

Electronic Business

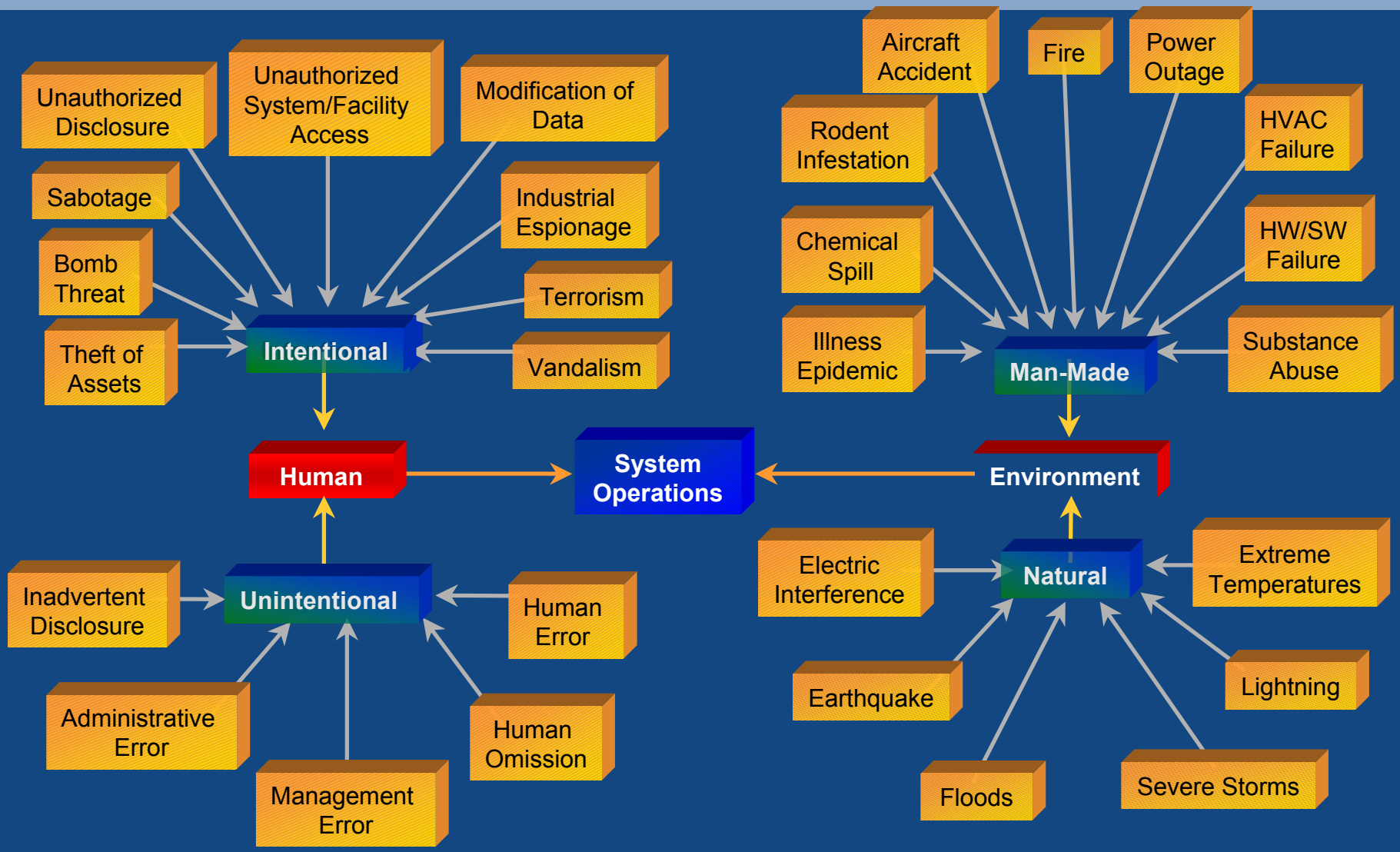
Vulnerabilities over Untrusted Networks



A Risk Framework



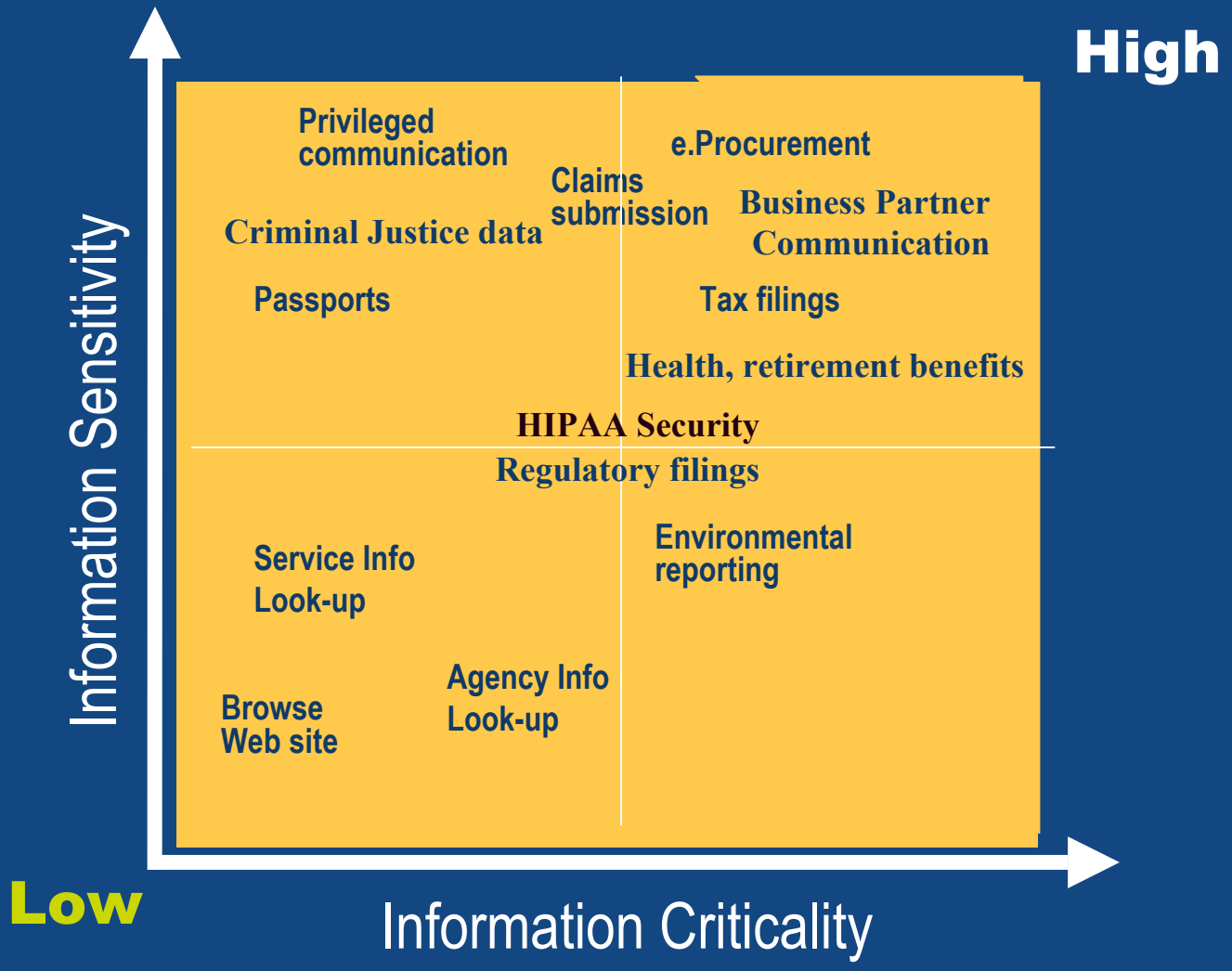
Threat Model



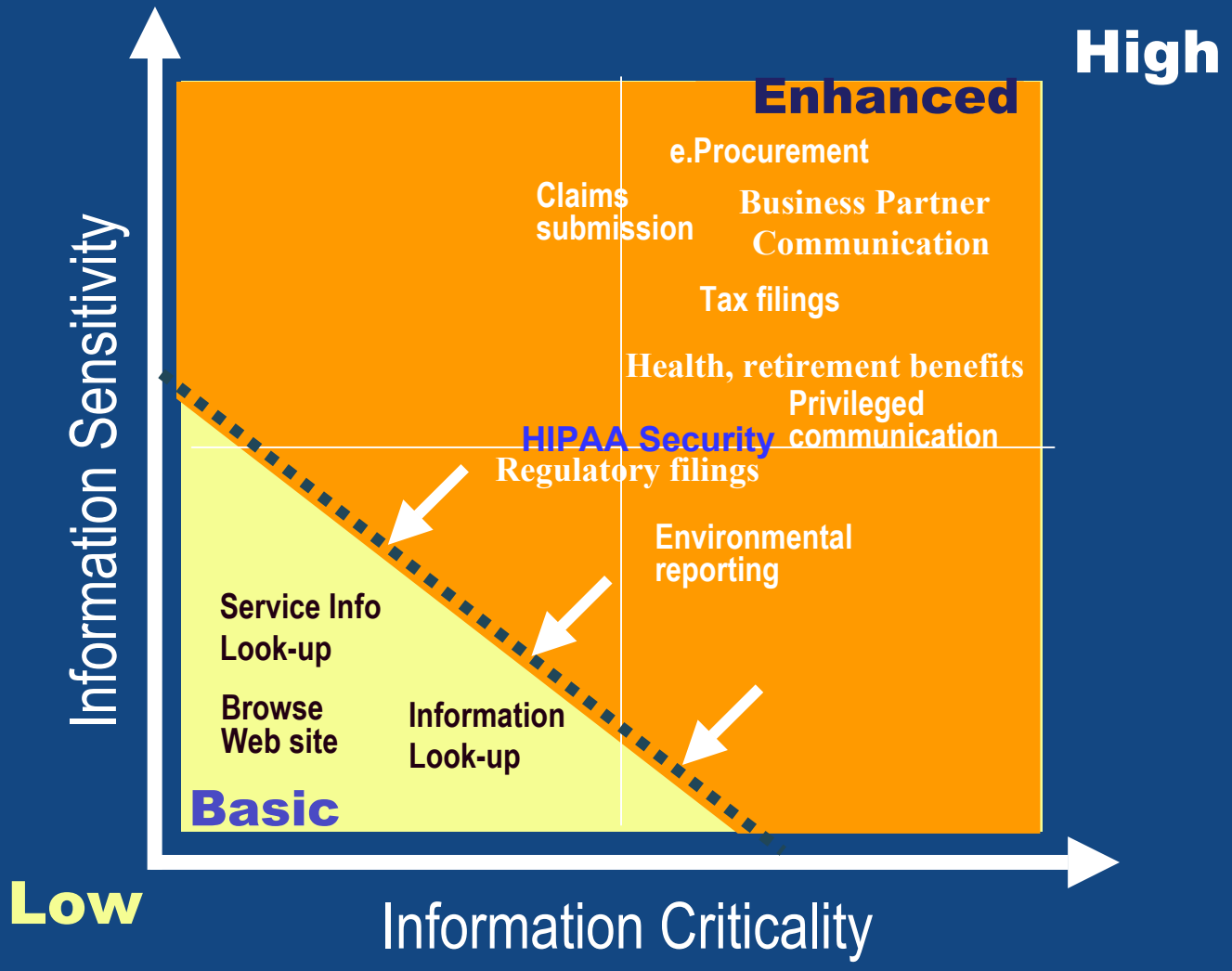
Risk Levels


Unacceptable - Risk cannot be tolerated
As Low As Reasonably Possible
Tolerated only if risk reduction is impractical or grossly expensive
Acceptable region
Negligible Risk

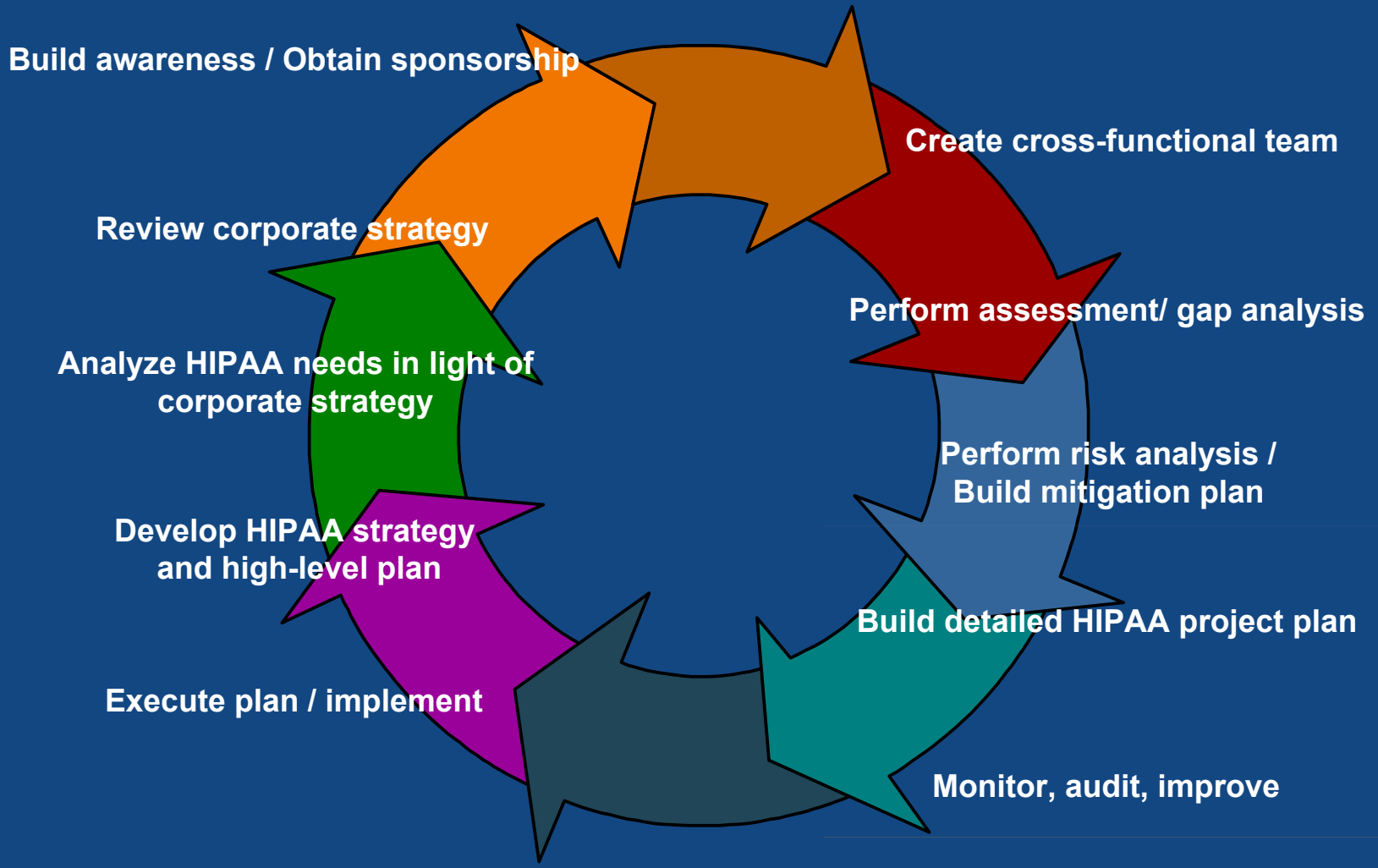
Trusted Business Model



Trusted Business Model – Current Status

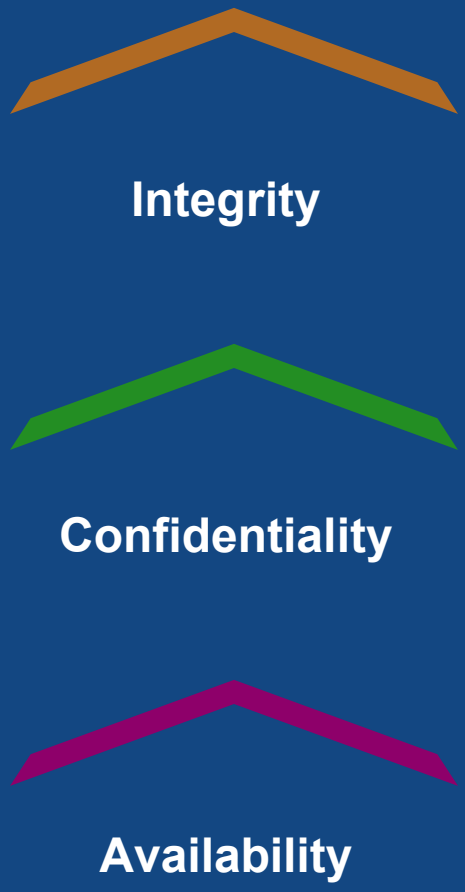


HIPAA Approach



24 HIPAA Security Rules

- Administrative Procedures
- Physical Safeguards
- Technical Security Services
- Technical Security Mechanisms



Best Practice Foundations

- ISO – 15408, 17799
- DoD – DITSCAP, Rainbow Series,
- ASTM – Health Information Standards
- NIST – SP 800 Series
- FIPS – Federal Information Protection Standards
- OMG – Corba, XML
- CMS – Internet Policy
- FDA 21 CFR Part 11 – Electronic Records-Electronic Signatures Final Rule
- IEEE – Electrical/Electronic Standards
- IETF – Internet Standards
- IATFF – Information Assurance
- CPRI-HOST - Templates
- Carnegie-Mellon – SSE CMM
- DRII – CONOPS, DRP
- CEN – European Pre-Standard Medical Informatics

Two Key Best Practice References

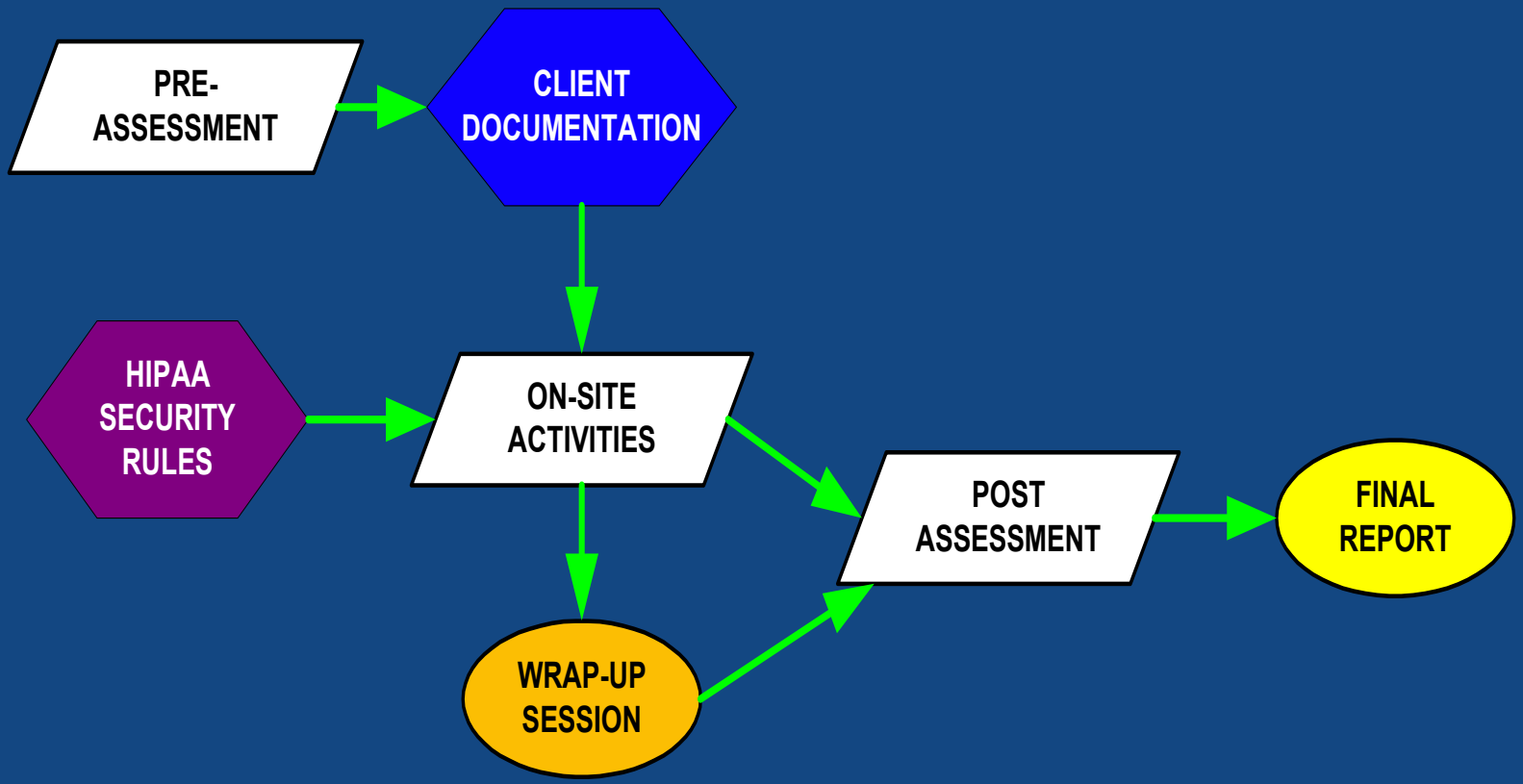
- NIST SP800-12 – introduction to computer security (the NIST handbook)
- NIST SP800-14 – generally accepted principles and practices for securing information technology systems

http://niap.nist.gov

Steps to Understanding your HIPAA Security Profile

1. Identify your information elements and modalities.
2. Prepare information criticality matrix. Determine extent of risk for each element relative to confidentiality, integrity, availability, accountability, and non-repudiation.
3. Define information security boundaries: topology as well as operational responsibilities.
4. Interpret the implications of each of the 24 proposed HIPAA security rules as they apply to your environment.
5. Evaluate your environment according to the requirements of the HIPAA rules for the information defined by the criticality matrix.
6. Analyze your findings relative to risk and compliance.

HIPAA Assessment Methodology



Compliance Scoring

Ratings are expressed in terms of current readiness as weighed against HIPAA requirements[1]

Scoring Scale	Definition
1	No identified process or control
2	Informal or partial process or control
3	Process or controls implemented for many required HIPAA elements
4	Process or controls fully implemented for all required HIPAA elements
5	Process or controls exceed required HIPAA elements

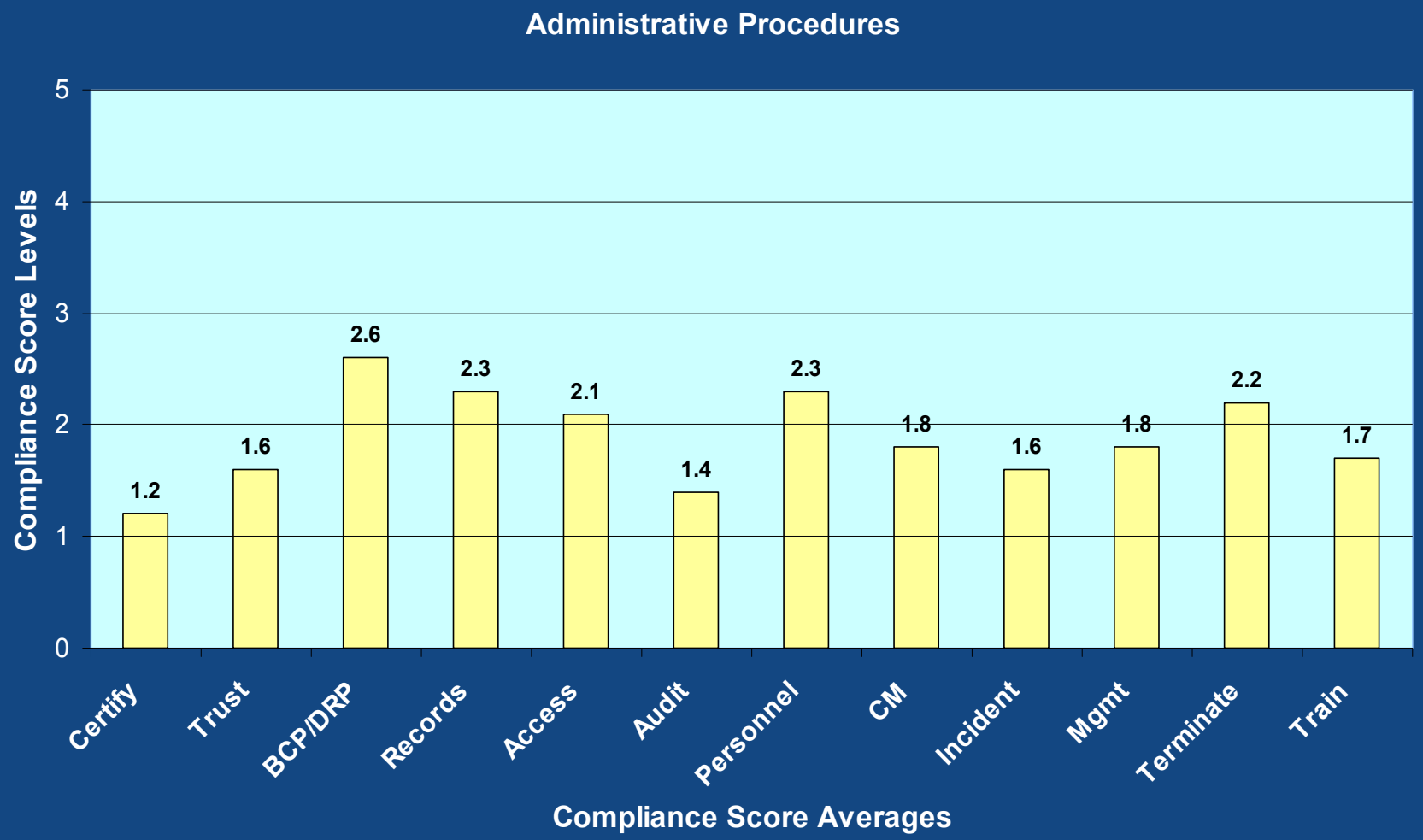
[1]Qualitative ratings derived from The HIPAA Security Summit Draft – HIPAA Security Summit Guidelines, Version 1.2. Baltimore, Maryland, June, 2000

12 HIPAA Security Administrative Procedures

1. Certification
2. Chain of trust partner agreement
3. Contingency plan
4. Formal mechanism for processing records
5. Information access controls
6. Internal audit
7. Personnel security
8. Security configuration management
9. Security incident reporting
10. Security management process
11. Termination procedures
12. Training

12 HIPAA Security Administrative Procedures

Observations from Compliance Assessments

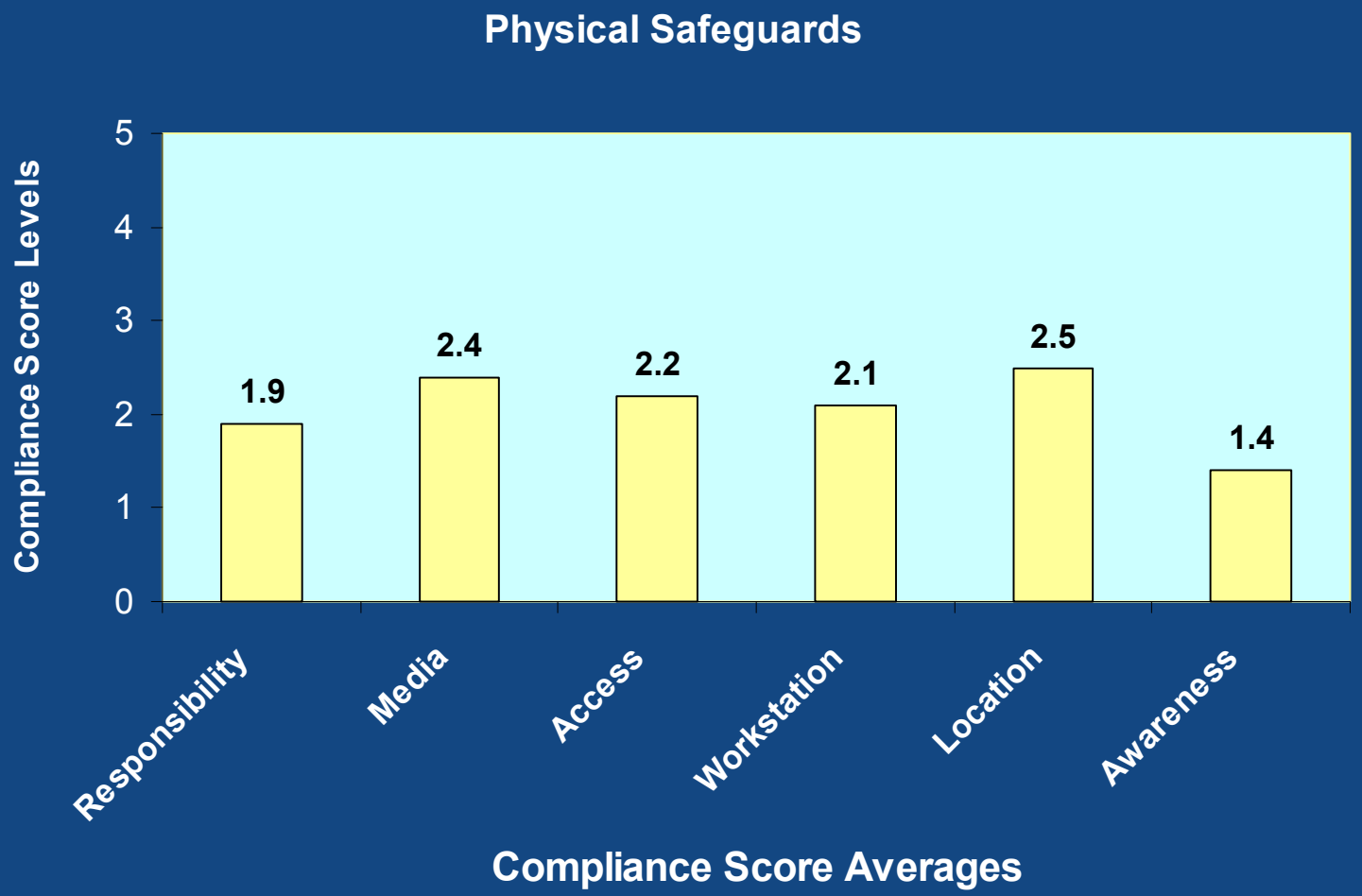


6 HIPAA Security Physical Safeguards

1. Assigned security responsibility
2. Media controls
3. Physical access controls
4. Policy/guideline on workstation use
5. Secure workstation location
6. Security awareness training

6 HIPAA Security Physical Safeguards

Observations from Compliance Assessments

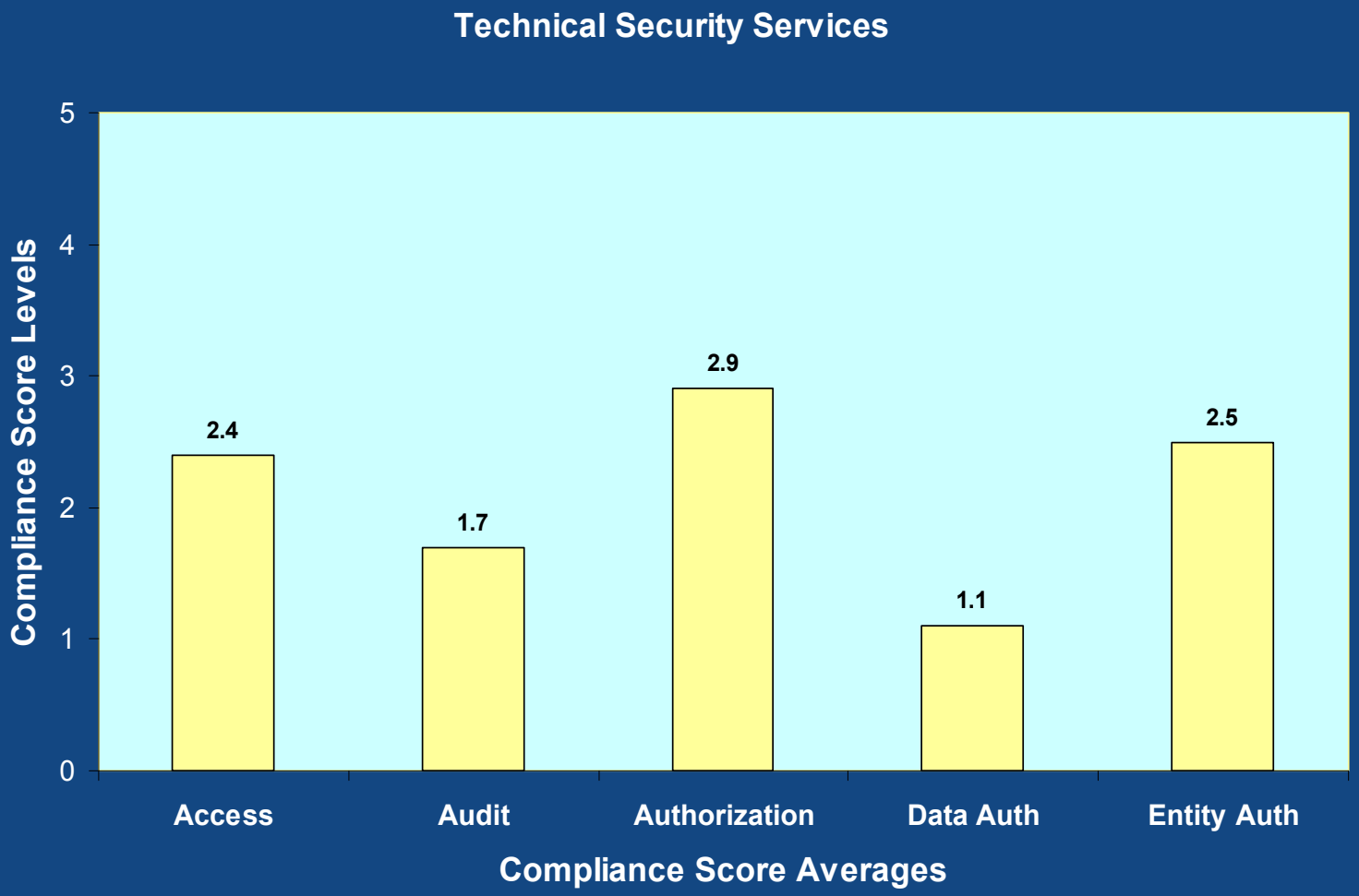


5 HIPAA Security Technical Security Services

1. Access controls
2. Audit controls
3. Authorization controls
4. Data authentication
5. Entity authentication

5 HIPAA Security Technical Security Services

Observations from Compliance Assessments

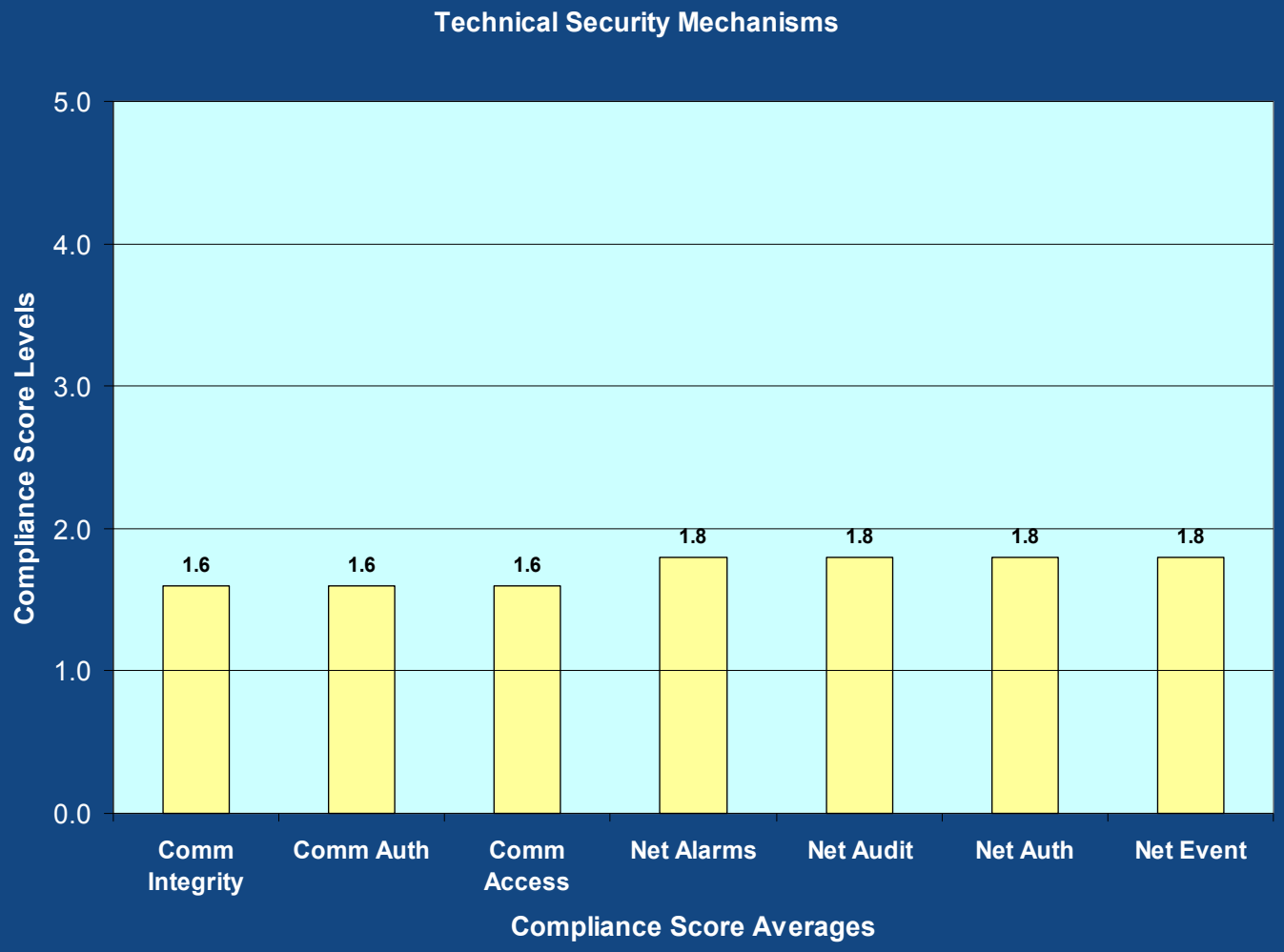


HIPAA Security Technical Security Mechanism

- Communications controls
  - Integrity controls
  - Message authentication
  - Access controls
  - Encryption
- Network controls
  - Alarms
  - Audit trails
  - Entity authentication
  - Event reporting

HIPAA Security Technical Security Mechanism

Observations from Compliance Assessments



Steps to Achieving and Maintaining HIPAA Compliance

1. Define your Corporate Strategic Vision.
2. Define your Information Security Strategic Vision (SSV). Interpret your corporate strategic vision as it pertains to managing information security risk and HIPAA security compliance.
3. Align your Information System Security Policy (SSP) to your SSV.
4. Define corporate information security standards that interprets the SSP for each electronic information modality.
5. Prepare Information Security Procedures that comply with the SSP and security standards.
6. Conduct GAP analysis of HIPAA findings with SSP and procedures.
7. Conduct risk analysis and prepare implementation plan.
8. Execute plan.
9. Monitor, audit and improve.

Promotes Consistency, Interoperability

- Economies result from consistent implementations
- Interoperable subsystems can be developed once and re-used across the enterprise
- Provides a basis for development of templates that can be re-used with minor modification to meet unique requirements
- Component interaction mechanisms can be separated from component configuration

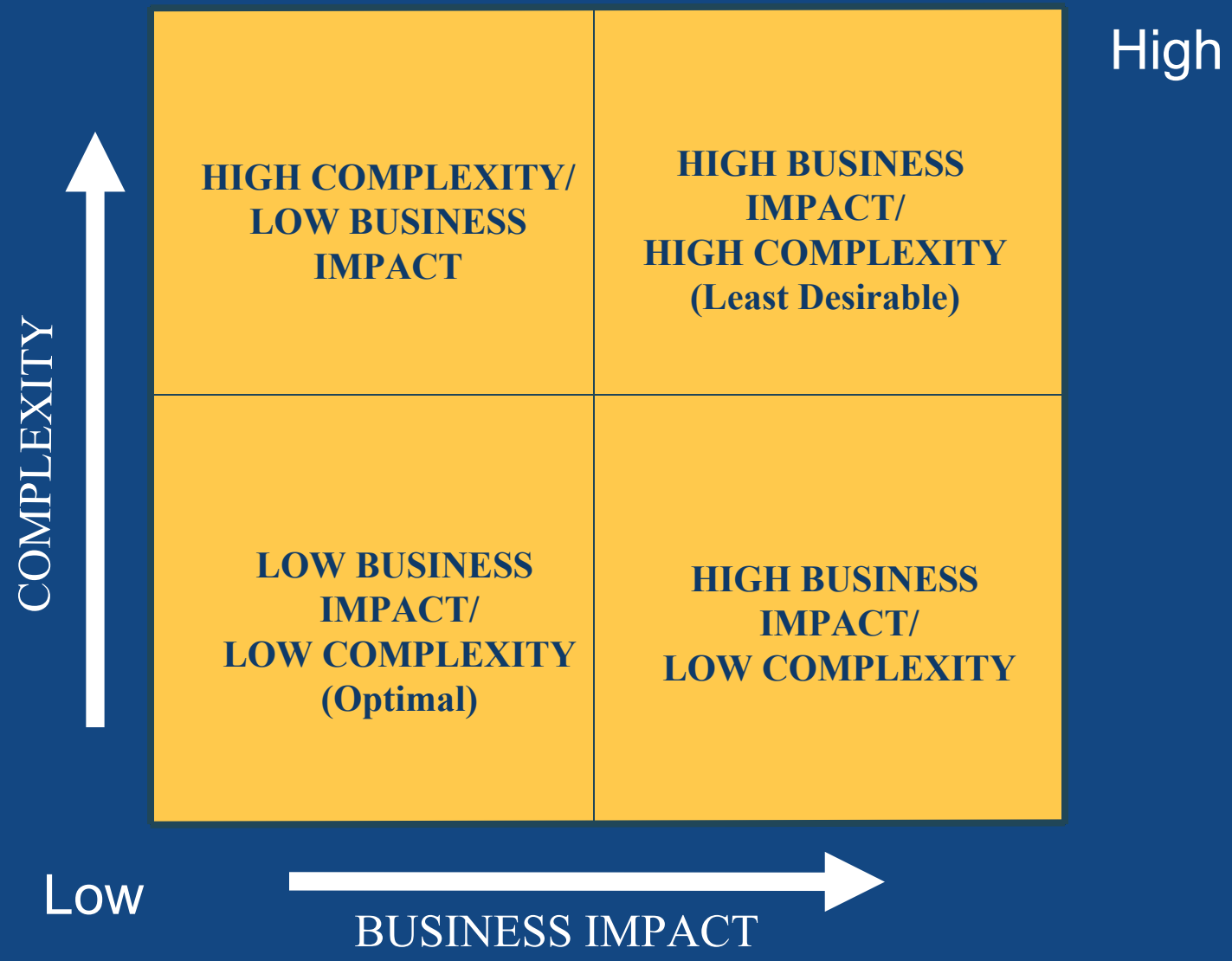
HIPAA Security Success Factors

- Involve Stakeholders
- Integrate Operational/Technical Architecture
- Define the Enterprise
- Define the Purpose
  - Reduce Cost of Security
  - Define Minimum Accepted/Expected Risk
  - Establish Expected Risk
  - Increase Competitiveness

HIPAA Security Success Factors

- Ensure Equity, Flexibility, Utility
- Distinguish Between Policy, Architecture, and Implementation
- Balance Enterprise Mission vs. Security While Striving for Measurable Improvements in Both
- Establish Verifiable Goals and Objective With Achievable Timeframes
- Is It Understood & Supported At All Levels Within the Enterprise

Privacy + Security = Confidentiality



Things to keep in mind….

- HIPAA Security is only part of the solution
- Electronic Information Security fosters the trusted environment necessary for e.Health
- Electronic Information Management requires changes to business practices
- Will require substantial investment in time and money
- Benefit from established Best Practices
- Security awareness is everyone’s responsibility
- Piece meal approach will not work
- Out-of-the-box solutions do not exist
- Security personnel must have proper training

Conclusions

- Patient information confidentiality requires both privacy and security solutions.
- There is no single “right solution”
- Organizational mission, sector, size and complexity will dictate the right mix of privacy and security solutions to meet HIPAA regulatory requirements.

Some Useful References

- http://csrc.nist.gov
- http://www.epic.org
- http://www.iatf.net
- http://www.sans.org
- http://niap.nist.gov
- http://www.ieee.org/
- http:// www.ietf.org
- http://mattche.iiie.disa.mil
- http://www.dr.org
- http://www.omg.org
- http://www.astm.org/
- http://www.contingencyplanning.com
- http://www.iso.ch/isoen/ISOOnline.frontpage

Just when you thought you had the "security thing" covered ...

Practice entry point:

- Mark Schuweiler, Director
  Healthcare, Insurance, Banking and Finance Information Assurance
- (703) 904-8975 mark.schuweiler@eds.com
- Global IAS Website:
  www.eds.com/information_assurance

EDS
solved.
eds.com